INTRODUCTION

This handbook is just one of the Pacific Bell *LockOn Services* that are designed to protect you from toll fraud. Toll fraud is unauthorized calls made through your telephone system, which means you end up paying for someone else's phone calls. Toll fraud affects businesses like yours every day. Whether you have a Key System, PBX, Voice Mail, Auto Attendant, or Call Diverter, your business may have long-distance calls stolen from you through fraud.

Pacific Bell's LockOn Toll Fraud Prevention Handbook is designed to help you prevent toll fraud. It helps you review and analyze your system, identify your vulnerabilities, and take preventive measures against misuse of your telecommunications system. To prevent fraudulent situations, you will probably need to take specific actions with assistance from your vendors or your Pacific Bell Account Team. So be sure to document your actions and requests for assistance. Then follow through to ensure that the appropriate actions have been taken.

Unfortunately, these are not the final steps you need to take. You must also maintain your vigilance, since criminals or hackers are constantly inventing creative, new ways to penetrate your system. Using persistence—and the information provided in this handbook—you can make it far more difficult for anyone to compromise and use your system.

Pacific Bell *LockOn Services* provides, at no charge, the centralized Fraud Bureau, which monitors call traffic routed through the Pacific Bell network. This bureau continually watches for warning signs that indicate potential fraud. Then you or your Account Team will be alerted if fraudulent calling patterns are detected. In this way, quick action can be taken to remove the perpetrator from your system.

If you suspect fraud is occurring on vour system you can call the Centralized Fraud Bureau on 1-800-953-5366.

Chapter 1

TOLL FRAUD: AN OVERVIEW

Toll Fraud Defined

"Toll fraud" is one of the most important issues of telecommunications today. Yet the term is relatively new, frequently misunderstood, and—until recently—was not an issue that directly affected Pacific Bell business customers. Now, however, our business customers need a working definition of toll fraud. That's because toll fraud has reached substantial proportions—and is a rapidly evolving cancer throughout the telecommunications field.

The telecommunications industry commonly defines toll fraud as: "The theft of long-distance services by an unrelated third party." The California Penal Code, Section 502.7 provides a more thorough, technical definition:

> ... any person who, knowingly, willfully, and with intent to defraud a person providing telephone or telegraph service, avoids or attempts to avoid, or aids, abets or causes another to avoid the lawful charge, in whole or in part, for telephone or telegraph service. This includes, but is not limited to, toll services and private networks, including 800 services ....

In this handbook our primary focus is on customer-provided equipment (CPE) toll fraud. With this type of fraud, long-distance service is stolen by penetrating privately owned CPE, then using the equipment to place unauthorized calls. The CPE may be a customer-owned switch or a Private Branch Exchange (PBX), Voice Mail System (VMS), Auto Attendant, or Automatic Call Diverter (ACD).

There are other types of toll fraud. They include:

- **Cellular Toll Fraud**

  The exploding cellular communications industry is a primary target of toll fraud. Thieves capture and duplicate the cellular user's electronic serial number (ESN) and mobile identification number (MIN) on a "new" cellular phone chip—which they sell. When the "new" chip is placed in the buyer's phone, long-distance calls are billed to the original chip owner's cellular phone.

- **Subscription Toll Fraud**

  False credit information is used to steal long-distance service from local telephone companies such as Pacific Bell and from long-distance carriers. At the start-up of service, usage is extremely heavy for a brief time. Then the "subscriber" disappears and the local telephone company and long-distance carriers are left with non-collectible bills. This method of theft continues to be a serious problem.

- **Calling Card Toll Fraud**

  Calling card numbers may be stolen when criminals, observing public telephones, watch unsuspecting victims dial in their calling card numbers. These "stolen" numbers are then sold to people who use the numbers to make "free" calls or to sell calls to others. Besides telephone observation, other known methods of obtaining calling card numbers include: retrieving the numbers from discarded records in dumpsters; manipulating unsuspecting secretaries to reveal the numbers by falsely claiming to be representatives of telephone companies; and by "finger hacking," where thieves who know a business number work out the remaining four digits to create a calling card number.

- **Distribution Toll Fraud**

  Criminals can penetrate the phone closet of an unsuspecting business and attach their own telephone hardware. Their calls are then billed to the owner of that business.

- **Employee Abuse**

  This is probably the most common and best known type of toll fraud. In this case, an employee uses the employer's phone system to place personal long-distance calls—which later appear on the company's phone bill.

- **Third Number Billing Fraud**

  There are many variations of this ongoing problem. Most commonly, a call is billed to a third number (generally a business number) without the knowledge or permission of that business.

Annual Cost of CPE Toll Fraud

It is difficult to estimate the annual cost of CPE toll fraud, which continues to spread and increase. Reliable "hard" figures are not available, largely because victims are reluctant to report these incidents and make them public. Embarrassment and potential liability with their customers are cited as factors for not filing police reports.

Through extensive research, Telecommunications Advisors, Inc. (TAI)[1] has developed a reliable estimate of the size of the problem. This information indicates, for example, that—at the $3 million dollars a day the long-distance carriers have indicated—toll fraud is at a level in excess of $1 billion per year.

Regulatory filings, court claims, and published reports through 1991 identify over 90 toll fraud victims—and the dollar amounts for long-distance usage/service stolen. For all reported cases, the average amount is $168,000—after excluding all incidents involving

$1 million or more. (This "average" figure is assumed to be higher than the norm because the occurrences that become part of the public record probably involve larger thefts.) In California, the "average" amount per theft is decreasing, due to increased surveillance by long-distance carriers and Pacific Bell. Offsetting this reduction in amount, however, is the *increased number* of incidents.

Business losses due to toll fraud go far beyond the long-distance usage/service actually stolen. An accurate assessment of annual costs in the United States must identify all elements and arrive at a projected cost for each. For example, some instances of CPE toll fraud use the incoming 800 numbers of the business or organization to penetrate the system and initiate the actual theft. This use of the 800 lines, itself, is quite costly to the owner. Losses from toll fraud must also include the hours expended by a fraud "victim's" management and staff, by security and telecommunications experts, and by attorneys.

TAI's review of the actual yearly costs of toll fraud has been limited to the United States. The problem has spread throughout the world, however, and is becoming far worse in other countries, where less sophisticated equipment and security devices are the norm.

The six categories listed below represent the primary direct costs of CPE toll fraud. The following categories have been excluded from consideration: 1) the indirect costs of preventive and security measures; 2) incremental private and public network costs; and 3) the cost of disconnecting extensive 800 line systems following a theft.

CPE TOLL FRAUD COST ITEM	AMOUNT
Stolen long-distance usage/service	$1,800,000,000
Toll fraud 800 charges	350,000,000
Victim management and staff time	40,000,000
Victim consultant and attorney fees	11,000,000
Carrier and vendor management and staff	15,000,000
Carrier and vendor consultant and attorney fees	17,000,000
Total annual estimated cost of CPE toll fraud	**$2,233,000,000**

Liability for Toll Fraud

Until recently, toll fraud as we know it did not exist, and its growing intensity was not anticipated. As a result, technicians developed feature-rich telecommunications systems—while providing minimum security protection against toll fraud intrusions.

Until well into the 1980s, liability for toll fraud was, essentially, a network or system problem. Carriers owned and controlled the system itself, along with most of the connected equipment. When toll fraud occurred, its costs were absorbed, directly and indirectly, by the system. User liability was unheard of, and the problem did not affect users.

The present-day CPE toll fraud problem, with its issue of responsibility, developed later. It grew out of the divestiture of AT&T—and the introduction and ownership of many kinds of customer-owned premises equipment. Financial liability for toll fraud then fell to the customer or the owner of the equipment.

CPE Owner Liability

Today, anyone can purchase and install their own customer-premises equipment, after choosing from a wide variety of alternatives. With this purchasing power has come a change in the liability for toll fraud—from the long-distance carriers and the overall "network" to the owner/user of CPE.

The major carriers' tariffs explicitly place liability on the user/owner of CPE. The carriers have no control over, and usually no knowledge of, the type of equipment customers have installed. Consequently, the carriers have no responsibility for its penetration and misuse. It is the user/owner who has the opportunity and responsibility to maintain, control, and protect that equipment.

Ownership of sophisticated PBX systems has also been equated legally with ownership of house phones. The "house guest" court cases[2] have placed legal responsibility for toll charges on the equipment owner. Defendants in this group of cases claimed, unsuccessfully, that they should not be held responsible for unauthorized calls placed from their telephones by guests in their homes.

To date, user ownership of CPE has allowed long-distance carriers to argue successfully that the combination of the house guest cases—and the language set forth in their tariffs—make the user/owner responsible for toll fraud. The carriers argued that only the customer has control over what occurs in a home or business. This argument has prevailed—and the customer, therefore, is currently held liable for all resulting charges.

Evolution of Toll Fraud

Because toll fraud probably began with collect call abuse, it has also been called Code Calling.[3] This form of long-distance service theft continues today as, for example, when two parties agree on key words that carry a particular meaning. For instance, a Lt. Col. Smith is sent to a foreign country on assignment. He needs to notify his headquarters that he has arrived safely. As prearranged, the Lieutenant Colonel calls his headquarters "person to person," or collect, and asks for Lt. Smith. The call is not accepted at headquarters, where the term "Lt. Smith" is recognized as a code— meaning Lt. Col. Smith has arrived.

Although the information has been relayed, the operator terminates the call—which means no one is charged. Since the customer does not pay appropriate charges, it is a form of toll fraud. Any information can be coded in this way, with codes distributed to those involved. As a result, this form of fraud costs phone companies enormous sums each year in added labor costs.

More technical methods of committing toll fraud evolved from collect call abuse. Devices known as "blue boxes," "black boxes," and "red boxes" and combinations thereof were developed, using known technical attributes of the telephone system. Among other capabilities, the devices could emulate signals and the deposit of coins into pay telephones. Technological advancements have largely defeated this form of toll fraud.

The evolution of this type of fraud brought about a generation of "techies" with a fascination for penetrating equipment and beating the system. Originally referred to as "Phone Freaks," and later "Phreaks," they are now often called "hackers." Extremely adept at using technology, they characterize themselves as explorers and pioneers. Although they routinely steal long-distance service, not all engage in these activities for commercial gain. Instead, they are largely motivated by the thrill and challenge of learning how to defeat new security systems.

While it would be inaccurate to characterize all hackers as mercenary professionals, a hacking subculture has developed that directly and indirectly helps fuel toll fraud. From this subculture, a few graduate each year into the "Big Leagues" of organized criminal theft and resale of long-distance usage/service. Hackers' services and technological expertise are purchased by organized criminal rings that need such talent to maximize profits. Security professionals advise that experienced hackers can command up to $10,000 a week in unreported cash for their services.

- **The Hacker's Credo**

  Hackers earnestly believe that all programs and information should be in the public domain. Craig Neidorf, in his magazine Phrack pronounced "knowledge is the key and it is FREE. The telecommunications and security industries can no longer withhold the right to learn, the right to explore, or the right to have knowledge."[4] Another hacker reportedly stated "It's okay to do anything in the name of learning as long as you don't cause harm. You have the right to access any information that can be accessed (through your technique). We also feel if they're not smart enough to stop us, we have the right to keep doing anything."[5]

- **A Hacker's Objective**

  A hacker penetrates systems for a variety of reasons: a burning desire to learn more about phone company operations, switches, computers and relays; a thirst for more knowledge about new computer programs developed by Bell Laboratories or other organizations; or for financial gain by obtaining access codes for resale to call-sell operations.

- **Electronic Bulletin Board Systems**

  Hackers are like big game hunters. They need to exhibit their trophies. Once a hacker has obtained information, a program, or an access code number, he wants a place to publicize his accomplishment. The electronic bulletin board system (BBS) is the location of choice for the hacker to display his trophy. A BBS is a set of files or databases which are stored on a host computer that can be accessed by a remote computer via an attached modem.

Electronic bulletin boards have become the modern "street corner" where hackers and electronic thieves gather to exchange information. Authorities have shut down BBSs that posted information for pedophiles, drug dealers, and those who deal in stolen access codes. Hackers may use legitimate BBSs as well as pirate, or hacker BBSs. Hackers use a BBS to post newly obtained access codes, credit card numbers, or more information on how to penetrate voice mail or PBX systems.

First Amendment Issues

According to the U.S. Supreme Court, the First Amendment strongly disfavors the imposition of prior restraint on free speech.[6] However, the First Amendment does not give someone the right to publish illegally obtained information. If a BBS operator knowingly publishes or encourages others to post illegally obtained access codes or credit card numbers that can be used to commit other crimes, that operator can be criminally liable. The issue, however, is a difficult one for the courts to apply in many instances. Despite common knowledge that some BBSs are used to exchange information that is later used to commit toll fraud, successful prosecution has been extremely difficult because of First Amendment safeguards.

Information and programs are costly to develop—and are valuable to the people who developed them. Some stolen information also includes credit histories or credit card numbers.[7] Information like this is private and never intended for public disclosure.

The Drug Culture and organized crime connection

Needing phone lines that are difficult to trace, criminals are acutely aware of law enforcement's increased use of "wire taps" on private and pay phone lines. They do not want their long-distance calls to be billed back to them, since that would leave incriminating evidence. Many criminals use altered cellular phones to make calls. Others use normal phones, but charge the call to someone else's credit card number. Criminals concerned about calls being traced prefer to use complicated routing, whenever possible. This means using a procedure called "looping" to place calls through two or more PBXs or VMSs—before the call is connected to a cohort here or in another country.

Routing calls through a PBX or VMS requires an access code for each system. This has created a thriving business for those inclined to obtain access numbers, because the codes bring large sums of cash. Authorities believe drug dealers, drug importers, and other criminals account for a sizable percentage of toll fraud. Many fraudulent calls are placed to such countries as Colombia, Panama, Venezuela, Guiana, Egypt, Burma, India, Pakistan, China, Russia, and the Caribbean nations.[8]

At one time, hackers and resellers worked independently. A hacker would break a code and, at no charge post the new number on a BBS. The reseller would check the BBS for fresh numbers and try any that were found. Now the drug dealers and other people organizing call-sell operations (the industry term for those who "retail" stolen long-distance services) are working in cooperation with the hackers, and are increasingly putting hackers on their payroll with salaries up to $10,000 per week. Call-sell operations need a continuous fresh supply of new access numbers, their stock in trade. Without them, a call-sell operation is out of business. Criminals hire the smartest computer techies in their area and provide them with the latest equipment. Some pay the hacker for each code obtained, a "piece-work" approach that puts the economic incentive on results.

These organized criminals have virtually unlimited financial resources. They can afford to put hackers on the payroll, provide the best hacking equipment, and buy CPE manuals. Armed with these manuals, the hacker can quickly learn the default passwords, and all the technical information for that CPE. With this information, it is easier to penetrate a system and steal access codes or install a "backdoor" through which the operation can enter a system and make fraudulent calls.

Drug dealers have penetrated voice mail systems and used them to buy and sell drugs. VMSs are popular with thieves because the system can handle a large amount of information—and the information can be updated from a remote location. In addition, the system allows users to hear a familiar voice. Drug dealers can call a VMS and give a coded description of drugs they have for sale. Buyers then call into the same mailbox and place an order. The drug dealer calls in regularly, collects orders, and the drugs are delivered to a predetermined location. A North Carolina utility company was the victim of CPE fraud perpetrated by drug lords. During a 13-day period in 1989, authorities believe the Medellin Drug Cartel made phone calls primarily to Colombia and Nicaragua. Charges for those calls totaled $70,000.[9]

Hardware and Software for Hackers

- **War Dialers**

  One of the software programs hackers have developed—and use most—is an automatic dialer. This type of program became widely known through the movie, *War Games*. The star of that film is a teenage hacker who breaks into the NORAD computer under Cheyenne Mountain in Colorado Springs. He set his modem and computer program, a War Dialer, to automatically dial numbers and record those that connected to another computer. A War Dialer or Robodialer can make many calls in a short amount of time. It does not require monitoring, and transfers its results to a disk or a printer. The program dials numbers to determine which connects to a modem. If it records a "hit," the number is flagged and recorded in a file or printout. The hacker can review this file or printout at leisure.

Once the War Dialer has made contact with another computer, a short program can be easily developed to break any barrier codes that might be encountered. In late 1991, one carrier recommended that all users adopt 9-digit codes, suggesting that such an approach would protect against toll fraud. The suggestion, while well intended, was naive. In fact, programs are available and advertised in hacker bulletin boards that can break a 6- to 9-digit code in less than six hours. As modems and computers have become faster, longer codes are needed to maintain system security. Transmission and calculation speed are faster now than they were five years ago. Computer clock speeds and modem transmission speeds will continue to improve for the foreseeable future.

Tapping a Lucrative Market: Recent Immigrants

Millions have immigrated to the United States in the last decade, a large number of them illegally. Some immigrants cannot afford a telephone. Others who could afford a phone are in the country illegally and are fearful of providing the necessary personal information to get a phone. These immigrants form a willing and lucrative market for call-sell operations.[10]

A weekend visit to some neighborhoods in New York City can be enlightening. On one such visit, during a weekend night, TAI observed long lines outside two pay phones located at a busy intersection. At each pay phone, a gentleman with a stopwatch was clearly in charge. For a sum, the caller would be connected to any number, foreign or domestic. All transactions were in cash, with no questions asked. A limit of 10 minutes was forcefully maintained. The operation was run in a very orderly and efficient manner. Police would occasionally stroll by, and appeared impressed with the well-behaved people patiently waiting in line.

These operations usually run during weekend and evening hours, when CPE that is left operating has excess capacity. In one night, an intersection with two pay phones can generate thousands of dollars in unrecorded cash. Although New York City is the prime retail market for such operations, they are spreading. Miami, Los Angeles, Detroit, Chicago, and Phoenix are up-and-coming cities, and these organizations are well run. In one small operation, an overall manager took care of banking and payroll. One hacker generated "good" numbers for the group, and eight salesmen performed dual roles. When the system operated, during evenings and weekends, they timed calls, collected cash, and dialed requested numbers. In off hours, they circulated within ethnic neighborhoods, promoting the service by word of mouth or hand-delivered circulars, and providing information on hours of operation and locations.

The "Retailers" of Stolen Long-Distance Service

Pay phones are not the only outlets for call-sell operations. One operator set up a house in Queens, New York. The house had dozens of partitioned cubicles, each containing a telephone and a chair. People lined up outside the building to pay from $3 to $5 cash for each long-distance call. The customer told an "operator" in the house the number to be dialed. The "operator" placed the call and charged it to a stolen access code. Once the call was connected, the customer was directed to a phone.[11]

PBX and CPE owners can suffer dramatic losses through call-sell operations. One call-sell operation made more than $1.4 million through a single PBX during a four-day weekend. The average, however, is about $50,000 per day, and the PBX owner is responsible for the bill.[12]

A construction firm had New York Telephone install 12 phone lines in a trailer at their construction site. The firm paid a cash deposit, and the lines were installed. One month later, the firm abandoned its deposit and the site. The trailer had housed a call-sell operation with calls billed to a PBX belonging to an unsuspecting company in Harrisburg, Pennsylvania, among others.[13]

In one publicized case, a Chicago auto supply company incurred $140,000 in long-distance charges over a single weekend. The calls were traced to pay phones located at the New York Port Authority Bus Terminal.[14]

In still another call-sell scam, thieves outfitted a van with cubicles and sold long-distance cellular calls as the van was driven around the city. The van had a regular route to pick up and drop off their clients. This approach prevented authorities from filming the operation or triangulating the location of the fraudulent callers.[15]

TOLL FRAUD CENTERS: WHERE THE CALLS GO

Although industry investigators estimate that 80 percent of all toll fraud originates in New York City, TAI believes that percentage was less in 1992—as operations spread to other cities. While New York City remains the major center, Los Angeles and Chicago are becoming major rivals in call-sell operations.

In some neighborhoods of Brooklyn and the Bronx, the call-sell operator acts like the local phone company. Recent immigrants turn to these operators when they want to phone home. Drug lords use call-sell operations to make untraceable calls. Consequently, most long-distance calls made from these operations are to known drug countries, and to countries from which the U.S. has had many recent immigrants. The most popular toll fraud "drug" countries are Panama, Bolivia, Colombia, other South American countries, and Pakistan. The most popular "immigration" countries are the small nations, territories and possessions in the 809 area code region (the Caribbean), Mexico, South America, and Pakistan.[16]

[1] This report is taken from the Telecommunications Advisors, Inc. (TAI) two-volume reference work, *Toll Fraud and Telabuse* (1992). Used by permission of John J. Haugh, Chairman.

[2] See, e.g., *Belden-Bragdon v. AT&T* (Maine P.U.C. September 5, 1989); *Gaither v. Mountain States Tel. and Tel. Co. and AT&T Communications*, Case No. GNR-T-88-4, Order No. 22068 (Idaho P.U.C. August 12, 1988); *Amaral v. AT&T Communications, Inc.*, D.P.U. 87-53-I (Massachusetts D.P.U. July 1, 1987); *Lyons v. New England Tel. and Tel. Co.*, D.P.U. 19917 (Massachusetts D.P.U. September 14, 1981).

[3] Anderson, L., "Doing Time On The Telephone Line," *Security Management*, page 31 (July 1991).

[4] Denning, D., The United States v. Craig Neidorf, *Association for Computing Machinery*, page 24 (March 1991).

[5] *Washington Post*, "The Terminal Men," page 1 (June 24, 1990).

[6] See, e.g., *Near v. Minnesota*, 283 US 697 (1931); *New York Times Co. v. United States*, 403 US 713 (1971) (The Pentagon Papers Case).

[7] Barlow, "S.P. Crime And Puzzlement: In Advance Of The Law On The Electronic Frontier," *Whole Earth Review*, page 44 (September 22, 1990).

[8] *Crain's New York Business*, "Guarding PBXs Against Telephone Fraud," page T19, (July 22, 1991).

[9] Escobedo, D., "Hackers Costing Companies Millions In Long Distance," *Utilities Fortnightly*, page 10 (October 15, 1991).

[10] Lewyn, M., "Foiled On One Front, Toll Fraud Crooks Now Pick On PBXs," *Telephone Engineer and Management*, page 8 (March 1, 1991).

[11] "Toll Fraud," *Teleconnect*, page 40 (May 1990).

[12] Cook, W.J., Costly Callers: "Prosecuting Voice Mail Fraud," *Security Management*, pages 40, 43 (July 1991).

[13] Leibowitz, E., "Voice Mail Fraud," *Teleconnect*, page 26 (August 1991).

[14] *Crain's Chicago Business*, "Phone Fraud Holds Up Business," page T1, (October 14, 1991).

[15] Eckerson, W., "Users Paying Big Price For PBX Fraud," *Network World*, page 1 (October 29, 1990).

[16] Eckerson, supra note 15.

Chapter 2

PBX TOLL FRAUD

PBX remote access fraud is one of the more common forms of toll fraud. Direct Inward System Access (DISA), often referred to as "remote access," is a feature available in most PBXs. It allows employees off premises to dial into the company's PBX and access all user capabilities, including long-distance usage/service. Generally, employees use DISA to interact with a company extension or obtain access to less expensive long-distance lines, such as tie lines and WATS (Wide Area Telecommunications Service) lines. The feature can be used with local telephone service but is more often used with 800 service.

After dialing the remote access number, employees receive a prompt. In a single-level security system, the employee must then enter an access authorization code. In systems with multiple security levels, employees are generally prompted for a multi-digit barrier code.

For long-distance thieves, it's a simple matter to decipher access authorization codes, especially if they are short or predictable. Then, if there are no dialing restrictions on a code, thieves can place an unlimited number of long-distance telephone calls. Without proper audit trails, unauthorized calls can go unnoticed for months. Companies that own a PBX should take the actions listed below to protect against toll fraud.

Evaluate the Need for Remote Access

For any system, remote access is the most dangerous feature. Each user should evaluate its necessity. Then, the feature should be deleted—*unless* removal would have a severe adverse impact on company operations.

If the DISA function is not used, *it must be eliminated or blocked.* If the feature is simply left inactivated, hackers can penetrate a system and activate it. So be sure to modify the software and/or protect the system administration capability to be sure hackers cannot activate the DISA function. Then contact your equipment vendor to remove or block the DISA feature. Each vendor has a different method of eliminating or blocking the feature. If you must use remote access, then take the following steps to reduce your risks:

- **Use Maximum Digits for Codes**

  Assign the maximum number of digits allowable for all access authorization codes and barrier codes. Most PBXs will accept 10 to 18 digits. The mathematics are simple. A 7-digit code provides 10 million possible combinations compared with a 4-digit code that provides 10 thousand possible combinations.[1] The greater the number of digits, the greater the protection.

Do not use telephone extension numbers, employee identification numbers, Social Security numbers, anniversaries, maiden names, or first names for access authorization codes or barrier codes. All codes should be randomly generated by the company's system administrator, and employees should not determine their own codes. Do not use group or department codes. Each employee should be assigned a separate, distinct code that is neither consecutive nor sequential.

- **Use Multiple Levels of Security**

  Use a barrier code—an additional code placed in front of the access authorization code—as a second level of protection.

- **Change Codes Periodically**

  Change access authorization codes and barrier codes periodically (e.g., monthly) as a routine administrative function.

- **Deactivate All Unassigned Access Authorization Codes**

  Have your system administrator keep an independent log of all authorized employees and their access authorization codes. Then, once a week, all codes within the PBX should be compared with this log. Note any discrepancies and correct them immediately.

  Many employees don't know their own passwords or identification numbers, so the codes are not used. Any unused code should be deactivated—particularly codes assigned to former employees, summer interns, or other temporary employees. When these employees leave, deactivate their codes immediately.

- **Do Not Publish Remote Access Numbers**

  Never publish remote access telephone numbers. And if possible, use these telephone numbers during normal business hours for other business functions—for example, for telemarketing or other work that dials out of the company.

- **Terminate Access at the Third Invalid Code**

  You should limit the opportunity to break your PBX barrier code or access authorization code. Just modify your PBX software to terminate a call automatically after a third invalid attempt—or route the call to a switchboard operator. We recommend the switchboard option, because an intercept by a live operator will often deter intruders. It also allows the operator to monitor and record multiple attempts to access the system—an indication of attempted toll fraud. Instruct your switchboard operator to notify the system administrator if this occurs.

- **Limit Remote Access During Non-Business Hours**

  Be sure to restrict or block the remote access capability during non-business hours. Just use the "time-of-day restriction" feature found in nearly all PBX software.

If 24-hour remote access is required, use the "automatic route selection" feature. During non-business hours, this routes all remote access calls to the switchboard operator—which can deter thieves. A system of regularly revised verbal passwords can identify a caller as a legitimate employee of your business.

- **Limit Your 800 Number**

  If you use 800 service for remote access, limit that service to the geographical area your company really needs. If you do business only in the western United States, don't purchase eastern access. Another inexpensive defense against toll fraud is to include Call Detail Reports as part of your 800 service. Then review usage patterns often to watch for signs of fraud. Pacific Bell *Custom* 800 Call Detail Reports include the full 10 digits of the calling number and are provided as a free service. Pacific Bell *Custom* 800 also has features that allow you to receive incoming calls only from selected area codes and/or specific prefixes.

- **Do Not Use Steady-State Dial Tone to Prompt Remote Access**

  Avoid using a steady-state dial tone as a remote access prompt. Thieves use automatic dialing programs to dial large blocks of telephone numbers. They record those numbers that give a remote access prompt, a modem prompt, or a VMS prompt. Use of a voice recording or silent prompt defeats the automatic dialing program. Most PBXs today can be re-configured to provide this capability. Request that your vendor do so.

- **Use Ring Delay Option**

  Most automatic dialing programs automatically disconnect after the second or third ring and move onto another telephone number. Therefore, a ring delay option should be used on remote access lines to deter potential thieves. Usually this option is set for four or five rings before the PBX answers the call.

- **Restrict Individual Calling Capability**

  Restrict individual employee calling capability. Assign restriction levels in the PBX based upon employees' business needs. Few individuals need access to international long-distance service. Most employees need access only to specific regions or specific states. Alternate restriction levels should be assigned to each access authorization code to restrict long-distance calling during non-business hours. If your PBX does not provide for this capability, you can use *Centrex* for your outgoing trunks. These trunks can then be equipped with features such as *Toll Diversion*. *Toll Diversion* and other *Centrex* features are described in detail in Chapter 9.

- **Toll-Restrict Outside Trunks and Station Lines**

  We strongly recommend that you restrict international calls and calls to the 809 area code (the Caribbean), *unless* you routinely do business there. With most PBXs, you can restrict all international calls—and restrict calls to selected area codes. There are still two potential risks, however: (1) The PBX software might fail to implement the program change for any number of reasons; or (2) An intruder or a dishonest staff member or technician could reverse the restriction. So be sure to test these restrictions often.

Take special care when restricting calls to the 809 area code, the destination for a high proportion of all fraudulent calls. Note that some locations within the area code, such as Puerto Rico, are *not considered international*. So simply blocking international calls is insufficient. Be sure to block the 809 area code specifically. Furthermore, as a second line of defense, using *Centrex Toll Restriction* (see Chapter 9) for your outgoing lines allows you to restrict calls to specific area codes or prefixes.

In addition, restrict 10XXX casual calling during non-business hours. And if possible, restrict tandem trunk and outbound 800 access during non-business hours. This reduces the risk of the PBX being used as a vehicle to penetrate another user's PBX.

For domestic long-distance service, program the PBX to block calls to area codes where you do not do business. In addition, area codes or prefixes that result in charges, such as 900, 950, and 976 should be blocked. And consider blocking, as appropriate, 411, 611, 10XXX, "0+", "0-", "00+", "00-" since these may be used to circumvent other restrictions you have put in place.

In some cities, the capacity of the 976 exchange has been exceeded, and additional "976 look-a-like" exchanges are being used. Be sure to block these exchanges, too, because they play a primary role in "pager toll fraud." In this form of fraud, thieves set up a pay-call service and leave the number on the pagers of your unsuspecting employees. Because "976 look-a-like" numbers are not generally recognized as toll calls, the employees return the call—and your company is charged.

"976 Look-A-Like" Exchanges to Block

Area Code	Area	976 Look-A-Like Exchanges
(202)	District of Columbia	915
(206)	Washington	960
(207)	Maine	940
(208)	Idaho	960
(212)	New York	540, 550, and 970
(214)	Texas	703
(215)	Pennsylvania	556
(216)	Ohio	931
(301)	Maryland	915
(303)	Colorado	960

"976 Look-A-Like" Exchanges to Block *cont.*

Area Code	Area	976 Look-A-Like Exchanges
(307)	Wyoming	960
(308)	Nebraska	960
(315)	New York	540, 550, and 970
(401)	Rhode Island	940
(402)	Nebraska	960
(410)	Maryland	915
(412)	Pennsylvania	556
(504)	Louisiana	636
(505)	New Mexico	960
(507)	Minnesota	960
(508)	Massachusetts	940
(512)	Texas	766
(513)	Ohio	499
(516)	New York	540, 550, and 970
(518)	New York	540, 550, and 970
(602)	Arizona	676 and 960
(603)	New Hampshire	940
(605)	South Dakota	960
(607)	New York	540, 550, and 970
(617)	Massachusetts	550 and 940
(713)	Texas	766
(716)	New York	540, 550, and 970
(718)	New York	540, 550, and 970
(719)	Colorado	898
(801)	Utah	960
(817)	Texas	892
(914)	New York	540, 550, and 970

- **Evaluate the Need for Using the Call Forwarding Feature From Your PBX**

  Determine whether you really need to forward calls to your answering service during non-business hours. Thieves can take advantage of the "click and pause" that occurs when each call is forwarded from your PBX. This pause allows time for them to hit the "0" button several times—which cancels Call Forwarding and also summons a long-distance operator. With the help of this operator—who believes the call comes from within your network—the thieves can make international long-distance calls. And your company receives the bill.

- **Use Effective System Audit Trails**

  Establish effective audit trails to monitor PBX access and usage. These provide daily feedback for system administrators to ensure that systems are running effectively. They also offer the first indicators that a PBX is experiencing toll fraud activity. This requires the PBX system administrator to monitor PBX traffic with "Station Message Detail Recording (SMDR)" and "Call Detail Reports" from the 800 service provider, and/or trunk activity reports generated by the PBX. System administrators can curtail toll fraud by checking these reports on a daily basis.

  Most PBXs are capable of generating data related to incoming and outgoing traffic through the PBX. These data, known as Station Message Detail Recording (SMDR), can easily be collected and stored for future analysis. Most PBXs have associated call accounting systems that correlate the data into useful PBX activity reports. However, even with a call accounting system, many PBXs are not equipped to detect irregular activities. There are a number of PC or mainframe-based call accounting system software packages available. The cost can range from a few hundred dollars to over a hundred thousand dollars. These systems can decode SMDR data and produce reports on incoming and outgoing traffic, and show such information as date, time, origin, and termination of the call.

  Larger users have the option of using a service bureau. Service bureaus electronically retrieve data from the company's PBX system and produce reports. They can consolidate traffic from switches at several different locations. Some service bureaus provide services aimed at identifying fraud, and provide exception reports that highlight abuse and suspicious activity. In addition, they will work with the users, carriers, and law enforcement agencies to document incidents for possible prosecution.

  SMDR data can be used to spot suspicious calling patterns and highlight unauthorized activity. It requires a baseline reading of your normal calling patterns/locations—which is used for comparisons that can identify later discrepancies. System administrators should watch for multiple short-duration incoming calls and long-duration outgoing calls. They should monitor PBX activity at off-peak hours such as evenings and weekends. Particular attention should be given to international long-distance calls. System administrators should also look for multiple failed attempts to access the PBX or multiple calls to unusual locations. Call Detail Reports from the 800 service provider gives system administrators valuable information about 800 service. System administrators should look for unusual increases in 800 line usage, a high number of calls from a particular number or area, and the caller's telephone number.

System administrators can also establish an internal company on-line Call Detail Reports data capability, allowing them to monitor PBX activity on a near real-time basis. Of all the system audit trail capabilities, this is probably the most responsive. But it requires an additional commitment on the part of the company in terms of money and manpower. Continuous in-house monitoring of the company's PBX operations requires either 24-hours-a-day coverage at the PBX control console, or an automatic alarm algorithm that can page a PBX attendant, who in turn can immediately shut down the PBX from a remote location. This approach allows employees to react immediately to any attempt to decipher codes or to unusual calling activity that normally indicates toll fraud.

Another weapon for system administrators is the verification and validation of telephone bills. As bills are received they should be broken down and disbursed to the applicable divisions, branches, and work centers for management to review and verify. Calls that cannot be verified as business oriented can be returned to the PBX system administrator and subjected to a company investigation to determine the source of the call.

- **Educate Employees About Remote Access Fraud**

  Company programs should educate employees about toll fraud. Employees who have access codes should learn that:

  - Codes are confidential business information.
  - Codes should not be written down on anything that may be discarded, lost, or seen by an unauthorized person.
  - Codes must not be shared with other people, even if the other person is an employee of the company.
  - Codes should be protected from observation when the employee is using pay phones at airports, hotels, bus stations, or similar locations.

Other types of Remote Access Fraud

Another type of remote access fraud is known to the industry as social engineering. A con artist places a collect call to a hospital claiming to be "Dr. Smith." If the PBX operator accepts the charges, the caller requests a specific department. When his call is transferred to that department, he tells the person answering the phone that he was incorrectly connected and asks to be transferred back to the PBX operator. To the PBX operator the call appears to originate internally. When the caller requests an outside line, the PBX operator may allow it. Again, the PBX owner pays for all long-distance charges incurred as a result of the caller's fraudulent phone calls.

Another toll fraud scam is the "just say yes" approach. In this approach, a call is made to a private party and the caller identifies himself/herself as an employee of the telephone company. They tell their prospective victim that the phone company is checking its circuits and that an operator will be calling in a few minutes with a third-party call. The caller asks the customer to "just say yes" to the operator and accept the third-party call. Most of the time, this works. The caller then promises the customer that the charge will not appear on their telephone bill and may even promise cash or credits to sweeten the deal. After talking to the customer, the con artist or an accomplice then places a long-distance call and has the operator charge the unsuspecting victim. This is a pervasive problem. **Pacific Bell never calls a customer to make this type of request. Should you receive such a request, refuse to comply.**

One way to prevent these types of remote access fraud is to order *Billed Number Screening** from Pacific Bell. *Billed Number Screening* does not allow collect and/or third-number billed calls to be made to incoming lines.

Prisoners often use a form of PBX fraud that we call "operator deceit." The inmate calls a PBX operator or a person with an access code and, using various ruses, gains access to an outgoing line or the remote access code. Any calls then made by the prisoner on a company's PBX will be charged to that company. If an inmate obtains a company's remote access code(s), he or she can make any call allowed by the company's PBX, including international calls. Besides making calls, the prisoner can also sell remote access codes. Others can then make fraudulent phone calls for which the company's PBX will be charged.

Annual reports and other corporate communications are often used by con artists to find a company's 800 number, and the name of a corporate officer. The perpetrator then calls the company switchboard, claims to be a corporate officer, and requests an outside line. The operator often complies and provides the service, thinking a favor is being given to a corporate officer. The perpetrator is then able to make any long-distance call allowed by the company's PBX, and the call is charged to the company.

In a specific case, an operator at a corporation received an inbound call from a thief—who claimed to be an important executive in the business. After chatting with the operator, he requested an outside line, because he "couldn't make an international call on his car phone." Trained to be courteous to executives, the operator immediately complied. In other instances, thieves have claimed to be representatives of the telephone network's security department, as a way to obtain access codes for long-distance services. In these cases, too, thieves have taken advantage of employees' courtesy and respect for "authority" to achieve their own ends.

Dumpster divers hunt through a company's trash bins looking for phone bills, corporate phone directories, and access codes—as well as other personnel or personal information that can be used to begin the hacking process. They can use many types of records with an employee's

* *When processing third-number and collect calls, some carriers do not use or access Pacific Bell's database containing the billing restrictions described. Therefore, it is possible for unauthorized third-number and collect calls to appear on your bill.*

name and credit account, e.g., credit card numbers appearing on a variety of receipts. Information on receipts retrieved from garbage cans can be used to make fraudulent calls.

Thieves may retrieve the name of a corporate telecommunications manager or departmental employee, and then use this information to manipulate another employee into revealing a code. For example, the thief will call someone in the company and identify himself as an employee of the telecommunications department. He will say that he is checking an account, and ask for the user's account number. If the user is suspicious and declines to reveal the code, the thief will ask for the last four digits only. Since the last four digits are the personal identification number (PIN) and the first 10 are the customer's telephone number, the thief then knows the entire code—and can make calls using the customer's full calling card number. This type of deception is increasing dramatically—and now takes many forms.

Toll Fraud Indicators

Toll fraud indicators are complex and contradictory at times. They can be broken down into two distinct categories: operational and statistical. Operational indicators involve situations which staff and customers encounter that suggest a potential problem. Statistical toll fraud indicators are revealed through PBX call accounting systems, voice mail administration reports, and trunk activity reports. The mere presence of one toll fraud indicator is not conclusive evidence of theft. Abnormal activity is often easy to explain. For example, a huge spike in outbound traffic may be triggered by an internal telemarketing campaign, or may result from a relatively simple anomaly. It should, however, serve as a catalyst for an immediate investigation.

Operational PBX Toll Fraud Indicators

- Staff difficulties in obtaining open long-distance lines or even local access lines.
- Customer complaints that lines are busy, particularly 800 lines. This can even have an impact on local access lines.
- Operator complaints about frequent hang-ups—or of callers expecting long-distance service.
- Operator complaints or comments that calls are frequently from individuals with foreign accents or poor English.
- Indications that lines are being used by strangers to converse in a foreign language.
- Attempts by outsiders to obtain sensitive information regarding the telecommunications system or calls from individuals posing as employees when they clearly are not.
- Any sign that the outgoing or inbound system is clogged or overloaded.
- A significant increase in the frequency of wrong number hang-ups.

- A significant increase in internal requests for operator assistance in making outbound calls, particularly international calls.
- Any calls from inside or outside the system claiming to be from important personnel and requesting operator assistance to dial international calls.

We recommend that you use statistical indicators for daily management of your telecommunications system—particularly for protection against CPE toll fraud. A sudden change in historical usage or calling patterns should be a red flag requiring prompt attention. Statistical data are best obtained through PBX call accounting systems, VMS administrator reports, 800 service Call Detail Reports, as well as trunk activity reports generated by CPE.

Every CPE system has different statistical capabilities and features. Software can easily be integrated within the system, if it is not already present. The type of data accumulated can vary widely, as well as the type of reports generated. A number of PC or mainframe-based systems can easily be used to enhance the statistical reporting capabilities of CPE.

Careful attention, preferably daily, should be given to the following statistical indicators of potential CPE toll fraud activity on a near real-time basis, through the implementation of a system that contains an automatic alarm algorithm.

Statistical Indicators of Potential CPE Toll Fraud

- Any sudden increase in 800 service usage that cannot be easily explained (e.g., an advertising campaign or other marketing promotion, or a seasonal variation).
- A sudden and significant increase in short-duration calls or frequent short-duration calls to a specific number, which is often indicative of an intruder using one system in an attempt to break into another system.
- The appearance of high-volume, long-duration incoming calls, particularly when associated with a similar increase in outbound long-distance service.
- Any significant increase in incoming or outbound calls during non-business hours (evenings, weekends, holidays).
- A significant increase in calls from a single geographical area or from the same number, or a sudden and unexplained increase in calling volume to a particular country, area, or exchange.
- Simultaneous multiple usage of an individual access authorization code in the PBX.
- A sudden increase in multiple failed attempts to use access authorization codes, barrier codes, and personal identification numbers.
- Traffic to unusual areas, particularly countries or area codes where the user does not normally engage in any business.
- Any unusual calling volume or change in calling patterns during non-business hours.

- Unusual tandem trunk-initiated incoming and outgoing calls through a PBX.
- Any unusual activity connected with known toll fraud regions, such as area code 809 (the Caribbean nations), Panama, Venezuela, Egypt, Guiana, Colombia, Burma, India, Pakistan, China, and Russia.
- Invalid attempts to enter the system administration port, which can occur through the dial-in capability or through an in-facility terminal.
- Any other unusual discrepancies in telephone bills, such as unusual calling patterns, calls to international destinations with which the user does not normally interact, and calls that cannot be accounted for.

[1] Carman, B., "Protect Your Network From Toll Fraud," *AT&T Newsletter*, page 9 (July/August 1991).

Chapter 3

VOICE MAIL TOLL FRAUD

A Voice Mail System (VMS) is an unattended answering service that records, stores, and retrieves messages. It can be used on a free-standing basis, connected to a PBX system, or off premises by a third-party vendor using the local telephone company's switching and trunk line facilities. These systems are a primary target of long-distance thieves, criminals, and industrial spies. It is often easy to defeat or bypass the system's security features and take over mailboxes within the system. Like many PBXs, VMSs have remote access features that make them extremely vulnerable to thieves. They have system administration and remote access capabilities through local access lines and/or 800 service. The remote access capability most often is integrated with the 800 service. Through the remote access feature, callers are able to receive and store their own messages and reroute messages to other voice mailboxes on the same system. These functions are manipulated by entering numerical commands via a telephone key pad in response to various computer prompts.

Security on VMSs is provided by PINs, which are used by customers to gain access to their voice mailboxes. PIN parameters are developed and controlled by the company system administrator (e.g., number of digits, frequency of change, etc.). Voice mailbox customers select their own unique PIN based upon parameters established by the company system administrator. To enter the VMS, callers dial the remote access number and upon receiving a prompt, dial in their respective PINs. If the PIN is valid, the caller gains access to a mailbox and its assigned capabilities.

Long-distance thieves attack VMSs in much the same way as PBXs. They dial blocks of 800 numbers, recording those numbers that give them a VMS tone prompt. Once they have identified the remote access number, they attempt to "break" customer or employee PINs. If they break a customer or employee PIN, they can take over that particular mailbox and use it for their own purposes, such as passing stolen PBX access authorization codes, stolen credit card numbers, computer passwords and call diverter numbers, and the telephone numbers and access authorization codes of other compromised VMSs. They also use the mailboxes to conduct other illegal activities such as drug deals, bookie operations, and prostitution rings. VMSs are also used by those engaged in industrial espionage. Industrial spies use VMSs to pass or steal confidential messages and/or leave bogus messages, to disrupt a company's operation.

If the VMS has an out-dial capability, it can be used by outsiders to place fraudulent long-distance telephone calls. The user must ensure that any associated out-dialing capabilities are removed or effectively blocked to prevent access to company long-distance and local services. Simply choosing not to activate the capability is insufficient; hackers can enter the system and activate it themselves. Therefore, we recommend this function be eliminated.

If there is an auto attendant feature available, ensure that the trunking associated with that system is restricted just as you would limit outbound trunking (900, 976, 809, 950, "0+", "0-", "00-", "00+", 411, 611 etc.) Thieves accessing the VMS through the remote access feature are, most often, using either local telephone numbers or 800 service. When asked to enter the desired extension, usually by the auto attendant feature, they enter 91XX or 9011. The VMS then attempts a transfer to that extension. To the PBX, this appears to be an outgoing toll call. The PBX connects the intruder to an outgoing line and the intruder dials the balance of the digits required. To protect a VMS, the user should take the steps listed below.

- **Use the Maximum Number of Digits for PINs**

  The PINs for all mailboxes should be set to the maximum number of digits. Fifteen is the ideal number, but in no case should the PIN be less than 12 digits. This should be required by the system administrator. Another alternative is to use 5- or 6-digit PINs in a tree system. Tree systems require mailbox owners to key in separate PINs to reach second, third, or even fourth levels of security. Although this is an alternative to consider if the VMS is penetrated, it should be used only as a last resort. The complexity of this system aggravates mailbox owners. With a 12- to 15-digit PIN, it should not be necessary to implement a tree system.

  If outsiders have unrestricted access to a company's VMS through an outside line, they can use an automatic code generator to break codes. To address this vulnerability, use the maximum number of digits possible. Telecommunications managers are often instructed not to lengthen PINs by company managers unwilling to deal with more than a 4-digit code. The conflict is between security and convenience. Convenience usually wins until the company is hit for a million dollars in fraudulent long-distance charges.

- **Randomly Generate All PINs**

  All PINs should be a mixture of letters and numbers in a non-sequential arrangement. They should be randomly generated under the supervision of the system administrator and *should not* be based on telephone extension numbers, employee identification numbers, Social Security numbers, anniversaries, maiden names, individual first names, simple patterns like 1-9-9-3, 1-2-3-4, 4-3-2-1, or the mailbox numbers themselves. Outsiders find it easy to identify, isolate, and use these types of codes.

  The system administrator should have the ability to change PINs if necessary. If a mailbox is compromised, the system administrator can then react immediately, cutting off the intruder. The system administrator should not allow the assignment of department or group PINs. Each mailbox must have its own unique PIN.